UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, -against- MARLEN RAPPA	14 Crim. 544

SUPPLEMENTAL SENTENCING MEMORANDUM ON BEHALF OF MARLEN RAPPA

Justine A. Harris
COLSON & HARRIS LLP
80 Broad Street, 19th Floor
New York, New York 10004
(212) 257-6455

Attorney for Marlen Rappa

Dated: New York, New York
April 1, 2015

I.

INTRODUCTION

Following the preliminary sentencing hearing held on March 13, 2015, this memorandum is respectfully submitted to address the Court's stated intention to depart or vary upwards based on the degree of the privacy intrusion involved in Mr. Rappa's offense. For the reasons that follow, an upward variance is not warranted, and Your Honor should instead sentence Mr. Rappa to a term of probation coupled with home detention, the bottom of the controlling Guidelines range.

First, as a matter of Guidelines interpretation, the facts of this case do not trigger an upward departure or variance based on the concerns outlined in application note 20(A)(ii) to U.S.S.G. § 2B1.1. The non-monetary harm caused by Mr. Rappa's offense was adequately accounted for in his Guidelines calculation and any further enhancement would be excessive and unwarranted.

Second, whatever the appropriate Guidelines analysis, the circumstances of Mr. Rappa's offense – [redacted] – warrant leniency, not an above-Guidelines sentence. Indeed, Mr. Rappa's conduct is distinguishable from those computer hacking or eavesdropping cases in which courts have imposed more severe sentences; moreover, sentencing him to less than what Kyle Fedorek received in no way creates an unwarranted disparity.

Finally, in determining an appropriate sentence, this Court should recognize that the Guidelines insufficiently account for Mr. Rappa's status as a first- time offender. Especially where, as here, a defendant's incarceration would devastate his family, both economically and emotionally, avoiding a lengthy period of incarceration is both just and serves the public interest.

II.

AN ABOVE-GUIDELINES SENTENCE IS UNWARRANTED BECAUSE PRIVACY CONCERNS ARE ALREADY ACCOUNTED FOR IN THE GUIDELINES CALCUATION

An upward departure is not warranted because the concerns expressed by the Court have already been addressed in the applicable Guidelines. First, Mr. Rappa stipulated to a two-point sentencing enhancement because his § 1030 offense involved an "intent to obtain personal information." U.S.S.G. § 2B1.1(b)(17)(A). This relatively new enhancement was specifically intended by the Commission to penalize the invasion of privacy, which may not be susceptible to monetization. Second, despite the fact that there is no concrete proof that any of the individuals affected by Mr. Rappa's actions incurred financial loss, he has also stipulated to a four point "victim" enhancement. Ordinarily, this enhancement is applicable only when people who "sustained any part of the actual loss" or "sustained bodily injury as a result of the offense" have been identified, and Mr. Rappa's stipulation to the enhancement recognizes the non-monetary harm he caused and factors that into the Guidelines. Cumulatively, these enhancements increase Mr. Rappa's Guidelines by six points, and any further enhancement is unwarranted.

A. Mr. Rappa Stipulated to an Enhancement for Intending to Obtain Personal Information, Which Fully Accounts For the Privacy Intrusion

At the March 13, 2015 hearing, the Court expressed the view that § 2B1.1, by focusing primarily on financial harm, does not adequately account for conduct where, as here, there was no quantifiable loss. (Transcript of March 13, 2015 sentencing proceeding ("March 13 Tr.") at 8) ("It's not really what the fraud Guidelines are dealing with, which tend to be much more driven by money and how much loss was caused. . . . the notion that it is a substantial nonmonetary invasion is not really taken into account by the balance in the Guidelines."). But the history of the Guidelines amendments suggests otherwise.

Admittedly, concerns over whether § 2B1.1's focus on financial loss failed to address non-monetary harm were originally addressed in the Guidelines' departure provisions. *See*, *e.g.*, *United States v. Spiegelman*, 4 F. Supp. 2d 275, 287-88 (S.D.N.Y. 1998) (Kaplan, J.) (noting that 2B1.1 "does not adequately measure the damage" caused by a theft causing loss "not fully measurable in economic terms" and relying on 5K2.5 for departure authority). In 1997, however, the Commission added an application note specific to § 2B1.1 advising that upward departures may be warranted where, "the loss determined under subsection (b)(1) does not fully capture the harmfulness of the conduct." U.S.S.G. § 2B1.1, App. Note 15 (1997). According to the Commission, an upward departure would be warranted in the case of "theft of personal information or writings (e.g., medical records, educational records, a diary) [which] may involve a substantial invasion of a privacy interest that would not be addressed by the monetary loss provisions of subsection (b)(1)." *Id*. In 2001, the Commission amended this § 2B1.1 upward departure guidance to substantially its current form. *See* U.S.S.G. § 2B1.1, App. Note 15(A)(ii) (2001).

However, the Commission subsequently and independently considered non-monetary harms – and specifically those harms resulting from theft of personal information – in the context of computer crimes. In 2002, Congress directed the Commission to review the Guidelines applicable to defendants convicted of computer offenses under 18 U.S.C. § 1030. *See* Cyber Security Enhancement Act of 2002, Pub. L. 107–296, 116 Stat. 2135, § 225(a) (2002). As part of its response to this mandate, the following year the Commission added U.S.S.G. § 2B1.1(b)(17)(A), providing for a two point enhancement if the "defendant was convicted of an offense under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information." "Personal information" was defined specifically to include non-financial but

nonetheless "private information involving an identifiable individual[,]" such as medical records, wills, diaries, e-mails, photographs of a sensitive or private nature, or similar information. *See* U.S.S.G. § 2B1.1, comment. (n.1).

In explaining the new enhancement to Congress, the Commission made clear that in the context of computer crimes, the two-point enhancement was a more appropriate way to penalize privacy intrusions than the departure provision in application note 20:

> Prior to this amendment, the issue of privacy had only been addressed in § 2B1.1 by way of an upward departure provision. . . . Although §2B1.1 does address privacy invasions with this discretionary upward departure provision, the Commission concluded that because of the increasing amount of sensitive personal information stored on computers, *a specific enhancement was the most appropriate way to account for harm resulting from computer offenses that compromise personal information.*"

United States Sentencing Commission, Report to the Congress: Increased Penalties for Cyber Security Offenses, at 11 (May 2003) (emphasis added).

Having crafted an enhancement for the theft of personal information, the Commission therefore narrowed the scope of Application Note 20, limiting its application in computer crimes to those cases where the non-monetary damage was particularly extreme. Simultaneously, the Commission added the following language to the text of Note 20(A)(ii): "An upward departure would be warranted, for example, in an 18 U.S.C. § 1030 offense involving damage to a protected computer, if, as a result of that offense, death resulted." *Id*. at 5, 13. Thus, the Commission concluded that, with respect to § 1030 offenses, only the most serious nonmonetary harms – akin to "death" – would warrant an upward departure. Certainly that is not the case here,

and thus the two point enhancement in § 2B1.1(b)(17) adequately penalizes the very serious privacy intrusion committed by Mr. Rappa.[1]

B. Mr. Rappa Stipulated To A Four Point Victim Enhancement Despite The Fact That There Was No Concrete Financial Injury

There is a second way in which Mr. Rappa's Guidelines calculation takes into account the non-monetary harm involved in his offense: it also includes a four point enhancement for the number of victims. *See* § 2B1.1(b)(2)(B) (plus four points for offenses involving "50 or more victims"). Mr. Rappa stipulated to this enhancement, even though under the Guidelines a victim is defined in relevant part as "any person who sustained any part of the *actual loss* determined under subsection (b)(1)." U.S.S.G. § 2B1.1, comment. (n.1); *United States v. Abiodun*, 536 F.3d 162 (2d Cir. 2008) (holding that people were not "victims" for purposes of victim enhancement where losses attributable to them were not included in loss calculation). Here, there was no "actual loss determined under subsection (b)(1)." Instead, the government has taken the view that some of the data stolen – photographs or music purchased by the victims from the internet – could have monetary value, even if nominal, and that hypothetically, individuals may have had to spend money to remediate any damage caused to their computers by the Blackshades malware. But such losses, while possible, have not actually been established, let alone "determined under subsection (b)(1)." *Cf. Abiodun*, 536 F.3d at 168-69 (persons could be victims where they suffered "loss of time" – time spent securing third-party reimbursement – but could not be counted among defendants' victims where their losses were not included in loss

[1] While some courts have applied the upward departure in cases involving harm less extreme than death outside of the § 1030 context, the invasion of privacy interests in those cases were on a massive scale. *See, e.g.*, *United States v. Rodriguez*, 443 Fed. Appx. 504, 2011 WL 4991605 (11th Cir. Oct. 20, 2011) (affirming upward departure in identity-theft sentencing under § 2B1.1 in light of substantial invasion of privacy resulting from defendant's illegal access to and theft of medical records of over 3,300 patients).

calculation). Mr. Rappa's stipulation to a four point enhancement of his offense level, despite the absence of any real financial damage or loss, is thus a relevant consideration for sentencing.[2]

Finally, the notion that there has to be an increase in the sentence for non-monetary loss commensurate with the loss table in § 2B1.1(b)(1) presumes that the enhancements based on loss are a meaningful sentencing schematic in the first place. But in fact, the loss table itself has been criticized as a poor measure of culpability, especially where other overlapping enhancements penalize the same conduct. *See*, *e.g.*, *United States v. Castaldi*, 743 F.3d 589, 598-99 (7th Cir. 2014)**.** Here, Mr. Rappa is already subject to six additional offense levels for the number of victims and the theft of personal information. Accordingly, the Guidelines calculation more than adequately accounts for the harm his conduct caused, making an upward departure inappropriate.

III.

THE CIRCUMSTANCES OF MR. RAPPA'S OFFENSE DO NOT MERIT AN UPWARD VARIANCE UNDER § 3553

Regardless of whether an upward departure is technically appropriate, the Court has indicated its intent "to impose the same sentence" – presumably an above Guidelines sentence pursuant to the § 3553 factors – whether or not application note 20 applies. But while Mr. Rappa's crime is serious, the circumstances of his offense in fact warrant leniency under § 3553, not an upward variance. First, sentencing Mr. Rappa to the bottom of the Guidelines would not

[2] None of the parties recognized the technical limitations of the "victim" enhancement until after the plea was negotiated. When counsel raised the issue with the government, pointing out that "victim" included only those victims who incurred financial loss, the government represented that while it could argue that there was at least nominal value assigned to the information obtained by Mr. Rappa, had the issue been raised before the plea agreement, the government would have insisted on defendant stipulating to an upward departure of 4 points, resulting in the same Guidelines range. Mr. Rappa, aware of the technical inapplicability of the victim enhancement, nonetheless abides by the terms of the plea agreement and the stipulation of the Guidelines range.

create any unwarranted sentencing disparities among the defendants already sentenced in the related Blackshades cases – *United States v. Fedorek*, 14 Crim. 548 (VSB), and *United States v. Sanchez*, 14 Crim. 333 (JCF).[3] Not only are there significant distinguishing factors between Mr. Rappa's case and that of Mr. Fedorek. The case of Mr. Sanchez, which was resolved with a misdemeanor and a one-year probation, more closely resembles Mr. Rappa's than the government has previously suggested. Second, while longer sentences have been imposed in other cases involving serious intrusions of privacy – unlawful surveillance or eavesdropping cases – those cases involved serious aggravating factors and public safety concerns not present here.

A. The *Fedorek* Disposition Does Not Justify an Upward Variance

At the March 13, 2015 hearing, Your Honor suggested that Mr. Fedorek's case was analogous to Mr. Rappa's, and that the fact that his Guidelines calculation was higher than Mr. Rappa's was the anomalous result of § 2B1.1's excessive focus on financial loss. (Tr. 13-15). True, Mr. Fedorek's higher Guidelines range was driven in large part by a six-point enhancement for the loss calculation (90 unauthorized access devices), but also relevant was the fact that he had infected more than 250 computers, which resulted in another six-point enhancement.[4] Moreover, whatever Mr. Fedorek's Guidelines calculation, the *below* Guidelines sentence he received – 24 months – should not be a baseline from which to measure Mr. Rappa's culpability.

[3] *See also United States v. Hogue,* 13 Crim. 950; *United States v. Johnston*, 14 Crim. 404; *United States v. Yucel,* 13 Crim. 834.

[4] Mr. Fedorek also received four points for having been convicted of 18 U.S.C. § 1030(a)(5). Indeed, in permitting Mr. Rappa to plead to the unauthorized access statute, 18 U.S.C. § 1030(a)(2)(c), the government tacitly recognized that there were distinctions between Mr. Rappa and Mr. Fedorek sufficient to warrant a four point difference in their respective Guidelines calculations.

Preliminarily, because Mr. Fedorek's 24 month sentence appears to have been driven in large part by factors extrinsic to the Blackshades charges. At the time of his arrest, Mr. Fedorek had pending drug charges in New Jersey. As Mr. Fedorek's counsel made clear at the sentencing, he had been offered a plea agreement in New Jersey to a "five flat," which "means in English, *that the defendant would be eligible for his release after two years*." (Fedorek Tr. at 14) (emphasis added). Counsel represented to the Court his belief that the New Jersey sentence would be imposed to run concurrently with the federal sentence. (*Id.* at 15). Thus, as reflected in the defendant's sentencing submission, defense counsel specifically *requested* that Judge Broderick impose a 24 month sentence, no more and no less. At the hearing, counsel explicitly stated that it was his hope to "fashion a sentence for him that will allow him to do all of his time in custody in a federal facility and *never have to endure either incarceration in a Bergen County facility or transportation from a federal jail to Bergen County for the purpose of a court appearance*, then to waste away for a while in Bergen County, and then to be transported back to a federal facility with all of the attendant hardship." (Fedorek Tr. at 14-15). Given that the defendant received a concurrent sentence crafted so as to ensure he did not have to serve any time in the harsher conditions of Bergen County jails, it is difficult to predict whether Mr. Fedorek would have received the same sentence had he not faced pending charges in another jurisdiction.

Beyond that, the amount of personal information Mr. Fedorek obtained far exceeded what Mr. Rappa retrieved in terms of quantity. According to the government, Mr. Fedorek infected at least 400 computers. Like Mr. Rappa, Mr. Fedorek obtained personal photographs from the victim computers. But in addition to these photographs, systematically organized on his computer were files containing: (1) 9,000 usernames and passwords for others' accounts,

including login information for electronic payment processors, banks, email accounts and social networking sites; (2) 50,000 credit card numbers, expiration dates and security codes; and (3) a "work" folder containing multiple other malware programs designed to obtain banking and other personal information from victim computers. (*See* Complaint in *United States v. Fedorek*, No. 14 Cr. 548 (VSB) ("*Fedorek*") (S.D.N.Y. filed May 15, 2014) (attached as Ex. A)). The evidence stored on Mr. Fedorek's computer was, in the government's words, "extensive and carefully organized," and the "level of organization and the variety of malware stored on Mr. Fedorek's computer" suggested that he was a "resourceful and determined hacker." (Govt. Sentencing Memorandum in *Fedorek*, attached as Ex. C).

While there was no concrete evidence that Mr. Fedorek actually used the stolen data to commit another crime, the nature of the information taken strongly suggests some intent or desire to commit fraud or to sell the data to others. Indeed, at sentencing, the government offered proof that when agents had searched Mr. Fedorek's room, they had found expensive items, including a 50 to 55 inch flat screen TV, a saltwater fish tank measuring the length of this bed, and a stack of $100 bills. (*See* Feb. 19, 2015 Sentencing Transcript in Fedorek ("Fedorek Tr.") attached as Ex. B). While it was unclear whether these items had been purchased with the proceeds of the Blackshades scheme or Mr. Fedorek's marijuana dealing, it certainly suggests that Mr. Fedorek sought to profit from his criminal conduct. Mr. Fedorek also did not have an unblemished record. He had convictions for DUIs and, at the time he was sentenced by Judge Broderick, was facing serious drug charges in New Jersey.

Here, both the circumstances of the offense, as well as Mr. Rappa's personal history, are worlds apart from Mr. Fedorek's. Mr. Rappa has no criminal record. Unlike Mr. Fedorek, before his involvement in Blackshades, Mr. Rappa had never violated the law. [redacted]

[redacted]

[redacted]

At bottom, the contrast with Mr. Fedorek's case is stark. While Mr. Fedorek was systemic and organized in his hacking, Mr. Rappa was disorganized and cluttered. The Blackshades program automatically created folders on Mr. Rappa's desktop, but many folders on his computer are practically empty, others have screen shots that are all black, and there appears not particular organizational system. Mr. Fedorek's residence showed off the latest technology and expensive hobbies; Mr. Rappa toiled away alone in his cluttered and messy garage office, while trying to launch a home printing office and care for and raise his twins. (*See* Photos of Mr. Rappa's home garage office, attached as Ex. F). Whereas Mr. Fedorek's use of Blackshades was part of a pattern of criminal behavior evincing a disregard for the law, Mr. Rappa's use was personal, haphazard and unconnected to any other criminal activity.

Indeed, in this respect, Mr. Rappa's case is more analogous to the case of Juan Sanchez. *See United States v. Sanchez*, 14 Cr. 333 (JCF) ("*Sanchez*") (S.D.N.Y. filed May 22, 2014). Like Mr. Rappa, Mr. Sanchez used Blackshades to access personal photographs and activate the webcam on the computer(s) he hacked. Thus, like Mr. Rappa, Mr. Sanchez received the two-point "personal information" enhancement under § 2B1.1(b)(17). Moreover, while the government asserted at the March 13, 2015 hearing that *Sanchez* involved only one victim, the defendant's ex-girlfriend, Mr. Sanchez in fact infected approximately 90 computers. Thus, he, too, received a four-point victim enhancement. [redacted] He was allowed to plead to a misdemeanor, and sentenced to one-year probation. (*See* Dec. 23, 2014 Sentencing Transcript in *Sanchez*, at 5, attached as Ex. E). Mr. Rappa, by contrast, will endure the lifelong stigma of a felony conviction and the widespread publicity surrounding his arrest and prosecution. Given that Mr. Rappa's culpability and mitigating circumstances place him between Mr. Fedorek and Mr. Sanchez, a non-jail sentence at the bottom of the Guidelines range, coupled with a felony conviction, home detention, community service and strict supervision, is sufficient to punish his conduct but take full recognition of the unique and sad circumstances that caused the offense.

B. Mr. Rappa's Case Is Not Analogous to the Unlawful Surveillance and Hacking Cases Cited by the Court

At the March 13, 2015 hearing, the Court referred to several unlawful surveillance and hacking cases that arguably involved similar invasions of privacy. While recognizing that those cases did present different facts, the Court stated that these cases illustrated, "what I think the criminal justice system is getting to, which is really that the harm is the invasion of privacy. . . ." (Tr. 28).

All the cited cases do involve violations of privacy, but the core sentencing considerations were aggravating factors unrelated to the privacy invasion, as well as serious public safety concerns. For example, in *United States v. Reithmeyer*, 426 F. Supp. 2d 893 (E.D. Ark. 2006), the court imposed a 36 month sentence – a substantial variance above the 6-12 month Guidelines range – for a defendant convicted after trial of four counts of wire interception, 18 U.S.C. § 2511(1)(a),[5] and acquitted of murder for hire and solicitation of a crime of violence. Specifically, the defendant was convicted of recording his soon-to-be-ex-wife's conversations on the telephone and in person during the course of an alleged conspiracy to gain custody of his children by planting illegal narcotics in his wife's vehicle and having her arrested on drug charges. *Id.* at 894.

Focusing on the devious scheme the defendant had concocted, the district court concluded an upward variance was warranted for three reasons: (1) the public required additional protection from defendant in light of his "cold-blooded determination to do whatever it takes to harm" his ex-wife and "wrest custody of their children from her," *id*. at 897 ("[w]hat brings us here are the foul means he employed — unlawfully taping Elizabeth's conversations and hiring someone to get her 'busted'"); (2) a Guidelines sentence did not adequately promote respect for the law in light of defendant's scheme to commit additional crimes in order to get his wife arrested on drug charges, *id*. at 897-98 ("The plot would have involved an abuse of the criminal justice system in order to subvert the legitimate operation of the civil system of divorce proceedings"); and (3) a Guidelines sentence did not afford adequate deterrence, *id.* at 898.

[5] This section provides civil and criminal penalties for a person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."

Specifically, the court in *Reithmeyer* relied heavily on the defendant's admission at trial of the scheme to frame his wife in order to obtain custody of the children: the defendant admitted he hired a bounty hunter nicknamed "Boston" to spy on his wife and, for that purpose, had provided Boston with pictures of his wife, her friends and relatives, and their children. *Id.* at 897 (noting that defendant "fully intended for [Boston] to plant drugs in [wife's] vehicle so that she would be falsely arrested and sent to prison."). In varying from the Guidelines, the Court repeatedly relied on this admitted relevant conduct, concluding that it "*goes far beyond the wire interception counts*" for which defendant was convicted. *Id.* (emphasis added).

The need to protect the public also was a central factor in *United States v. Hugh*, 533 F.3d 910, 911 (8th Cir. 2008). There, the defendant was convicted after trial of one § 2511(1)(a) count for tapping a private phone line during his efforts to locate a client of his wife's bail bond firm who had jumped bail. Concerned about the defendant's vigilante actions, the sentencing court imposed a middle-of-the-Guidelines sentence of 18 months. *Id*. Affirming the sentence, the Eighth Circuit noted the district court's finding that the Guideline range was reasonable, and highlighted the district court's reference to "the nature and circumstances here, the seriousness of the offense, the *deterrence here to other people not to boldly go out there and think that they have the law in their own hands . . . and to protect the public. . . ."* *Id.* at 913 (emphasis added).

Here, there is simply no corresponding need to protect the public. [redacted]

[redacted]

At the hearing, the Court also mentioned several state cases from the Appellate Division, Third Department: *See People v Piznarski*, 113 A.D.3d 166 (3d Dep't 2013); *People v. Stearns*, 39 A.D.3d 973 (3d Dep't 2007); *People v. Church*, 31 A.D.3d 892 (3rd Dep't 2006); *People v Evans*, 27 A.D.3d 905 (3rd Dep't 2006). These decisions all affirmed convictions and indeterminate sentences under New York Penal Law § 250.45, unlawful surveillance in the second degree.

While the New York unlawful surveillance statute may seek to punish some of the same conduct at issue here, these cases also involved aggravating factors. Three of the four state cases involve defendants who had abused positions of authority. *Stearns* involved a defendant employed as a caretaker for the disabled accused of taking pictures of one of his charges while she was unclothed. 39 A.D.3d 973 (3d Dep't 2007) (affirming sentence of one and one-third to four years' imprisonment). In *Church*, the defendant landlord pled guilty to ten counts of unlawful surveillance after police found a videotape containing nude depictions of ten women

living as tenants in defendant's buildings, along with audiovisual equipment allegedly used to install cameras in the victims' apartments and transmit images to defendant. 31 A.D.3d 892 (3rd Dep't 2006) (affirming aggregate sentence of 5 ⅓ to 16 years). *Evans* involved a defendant who surreptitiously placed a video camera in the bedroom of his girlfriend's 12-year-old daughter and recorded her undressing. 27 A.D.3d 905 (3rd Dep't 2006) (affirming sentenced of 1⅓ to 3 years).[6]

Moreover, in two of the cases, *Stearns* and *Church*, the defendants had engaged in similar conduct in the past and, therefore, arguably merited a stronger punishment. In *Stearns*, the prosecution introduced at trial prior bad acts, 39 A.D.3d at 974; in *Church*, the defendant previously had been convicted of aggravated harassment in the second degree "due to his threatened distribution of nude photographs of a former girlfriend." 31 A.D.3d at 893.

Unlike the defendants in these cases, Mr. Rappa had never previously engaged in similar conduct and did not abuse any position of authority or trust. Nor is there any evidence that Mr. Rappa, as in *Piznarski*, used any of the material he obtained to harass or extort any victims. While the Court has expressed the view that it is irrelevant that the victims may not have known about the privacy invasion, it plainly makes a difference that Mr. Rappa did not use the personal information to extort, humiliate or harass.

[6] The fourth case mentioned by the Court, *People v. Piznarski*, involved a defendant convicted after trial of four counts of unlawful surveillance in the second degree and two counts of coercion. 113 A.D.3d 166 (3d Dep't 2013). The conduct involved defendant's video recording of his sexual activities with two victims without their knowledge or consent. While not involving an abuse of status or authority, the defendant did abuse the trust of the victims. Moreover, the defendant engaged in the sexual extortion of one of the victims by "berating her and ultimately threaten[ing] to disseminate the video and humiliate her unless she agreed to have one final sexual encounter with him while he recorded it." *Id.* at 171. The defendant was sentenced to a prison term of 1 to 3 years imprisonment.

The facts of *United States v. Kazaryan*, No. 13-56 (C.D. Cal filed Jan. 25, 2013) ("*Kazaryan*"), make clear that such additional conduct would warrant harsher punishment. There, the defendant was charged under § 1030 with gaining unauthorized access to the e-mail, Facebook and Skype accounts of more than 100 victims. (*See* Indictment, attached as Ex. G). After gaining access to these accounts, the defendant allegedly changed the passwords (denying account-holders access), contacted friends of the account-holders and extorted those contacts into removing their clothing so that defendant "could view, and take pictures of, their naked or semi-naked bodies via their webcams." (*Id.* ¶ 1(i)). Kazaryan pled guilty to one count of aggravated identity theft and one count of unauthorized access in furtherance of criminal and tortious acts, 18 U.S.C § 1030 (a)(2)(C). Describing the defendant's scheme in its sentencing memorandum, the Government stated:

> [Kazaryan] methodically searched [victims'] accounts for naked pictures, passwords, and the contact information of their friends. . . . Once he had stolen the naked pictures from these women, he went further, returning to them in the guise of another victim account, and demanding that they provide him with more sexually explicit videos.

(*Kazaryan* Gov't Sent. Memo. at 1, attached as Ex. H). In imposing an above Guidelines sentence of 60 months, the district court explained that the Guidelines did not capture "the nature and extent of the way that this crime was committed and the human toll that it took on the victims by his egregious and terrorizing behavior." (*Kazaryan* Sent. Transcript at 51-52, attached as Ex. I).

While what Mr. Rappa did is wrong, it is a far cry from the cyberterrorstic acts engaged in by Kazaryan or the "sextortion" committed by Piznarski. Indeed, the Department of Justice has recognized that invasions of privacy are less serious where the private information is obtained solely for personal use, as opposed to being distributed to others. In a March 27, 2009,

letter to the Sentencing Commission commenting on proposed amendments, the Government discussed a high-profile case involving country singer Tammy Wynette. In that case, the defendant illegally accessed Wynette's confidential medical records and then sold them to a tabloid for publication. DOJ stated that, "disclosure virtually always increases the significance of the privacy invasion," noting that, "[i]t is one thing to obtain the medical records of an individual. It is quite another to disclose or publish that information."

Here, Mr. Rappa committed a serious breach of privacy. He deeply regrets his actions, is ashamed and full of remorse. As he writes in his letter to Your Honor, "Every day is a struggle for me to deal with the pain that I feel inside for the people whose privacy I invaded[.]" (March 6, 2015 Sentencing Memorandum, Ex. A). Still, as the facts of the cited cases demonstrate, it is nonetheless mitigating that Mr. Rappa at no time contacted the victims or sought to publish or distribute the information he obtained. Nor did he target particular individuals or threaten them. Given that first-time offenders who conducted unlawful surveillance to extort individuals or who abused positions of authority to gain access to and record private acts received sentences of 1-3 years or 1⅓ to 3 years, no upward variance is warranted here, where the breach of privacy remained personal to Mr. Rappa and did not involve the dissemination of that information or even threats to do so.

IV.

OTHER FACTORS MILITATE IN FAVOR OF A SENTENCE AT THE BOTTOM OF THE GUIDELINES

When setting up the Sentencing Commission, Congress directed that non-incarceratory sentences are generally appropriate for first offenders where the offense is not a "crime of violence or an otherwise serious offense. . . ." *See* 28 U.S.C. § 994(j). *See Mistretta v. United States*, 488 U.S. 361, 377, 109 S. Ct. 647 (1989) (relying on § 994(j) and other provisions to

conclude that, "although Congress granted the Commission substantial discretion in formulating Guidelines, in actuality it legislated a full hierarchy of punishment – from near maximum imprisonment, to substantial imprisonment, to some imprisonment, to alternatives – and stipulated the most important offense and offender characteristics to place defendants within these categories."). But in setting Guidelines ranges that call for jail sentences in the vast majority of cases, the Commission failed to fulfill the duty imposed by § 994(j). *See*, *e.g.*, *United States v. Leitch*, No. 11 Cr. 39 (JG), 2013 WL 753445, *1 (E.D.N.Y. Feb. 28, 2013) (the Commission avoided mandate of § 994(j) by "unilaterally declar[ing] in 1987 that every theft, tax evasion, antitrust, insider trading, fraud, and embezzlement case is 'otherwise serious,' and thus no more eligible for a sentence of probation, even when committed by a first time offender, than would a crime of violence."); *United States v. Watt*, 707 F. Supp. 2d 149, 158 (D. Mass. 2010). Thus, because the Guidelines in first offender cases are typically too severe, the Court should factor into its sentencing calculus Congress' judgment that a probationary sentence is "general[ly] appropriate[]" for first-time, nonviolent or serious offenders.

Notably, in *Watt*, the sentencing court factored § 994(j) in considering the appropriate sentence for the defendant computer hacker involved in "what is reported to be the largest conspiracy to commit identity theft in American history." 707 F. Supp. 2d at 150. The defendant was convicted of identity theft conspiracy for his part in a five year scheme in which he "adapted certain software that enabled the principals of the conspiracy to extract information from a number of companies. . . ." The scheme "resulted in millions of victims and substantial losses." *Id.* The Guidelines called for the statutory maximum of 60 months. *Id.* at 155. The district court imposed a sentence of two years, based among other facts on defendant's first-time offender status. *See id.* at 157-58 (noting that Commission's failure to implement § 994(j) led to a far

higher incarceration rate for non-violent first offenders, a result that "plainly does not comport with deterrence").

Here, for the reasons stated in Mr. Rappa's original sentencing memorandum, a Guidelines sentence of probation is appropriate. Mr. Rappa is a first offender and did not commit a violent or, as Congress defines, it a "serious crime." Since his release, Mr. Rappa has worked hard to turn his life around. [redacted]. Because it is his wife who works full-time, Mr. Rappa is often the primary caretaker at home and the bond he has with the twins is incredibly strong. Separating from them for any lengthy time would be traumatic, for him and for them. Beyond that, Mr. Rappa is deeply concerned that if he is incarcerated for any substantial period of time, his wife may lose the home and be forced to declare bankruptcy.

V.

CONCLUSION

There are myriad ways to punish an individual without sending them to jail. Given the unique circumstances that triggered the offense conduct, Mr. Rappa's first offender status and post offense rehabilitation, and the needs of his wife and two young children, I respectfully urge the Court to reconsider its stated intention to depart upwards and instead impose a sentence at the bottom of the Guidelines range.

Dated: New York, New York
April 1, 2015

Respectfully Submitted,

By: /s/

Justine A. Harris
COLSON & HARRIS LLP
80 Broad Street, 19th Floor
New York, New York 10004
(212) 257-6455

Attorney for Marlen Rappa